Security Architecture Work Group
Disaster Recovery and Business Continuity

Monday June 3, 2002
10:00 A.M. to Noon
NSOB 6X -- Lincoln

Minutes

A. Participants

Allan	Albers	HHSS
Rod	Armstrong	Nebraska Online
Mahendra	Bansal	Dept of Natural Resources
Dan	Davis	Nebraska National Guard
Dwayne	Dvorak	University of Nebraska
Scott	Evers	Dept of Labor
Steve	Hartman	IMServices
Ken	Hassler	Nebraska National Guard
Jerry	Hielen	IMServices
Bob	Keith	IMServices
Joe	Hinton	Nebraska Emergency Management Agency
Scott	McFall	Nebraska State Patrol
Steve	Rathje	Dept of Natural Resources
Leona	Roach	University of Nebraska
Steve	Schafer	Nebraska CIO
Ron	Woerner	Department of Roads

B. Review existing Policies, Activities, and Resources

Steve Schafer cited several sources of information relating to disaster recovery and business continuity planning. These include:

a. NITC Disaster Recovery Policy (http://www.nitc.state.ne.us/standards/index.html)
b. IS Technical Staff Template – Chapter 9 Disaster Recovery Rules (same website as above)
c. KPMG Management Letter to the NITC
d. Center for Digital Government – Briefing Sheet #4 Business Continuity in a Distributed Environment (see attached)

Other resources also exist such as SANS, NIST, and other states. The SANS web site (www.sans.org) offers several articles on disaster recovery in their reading room. A step-by-step guidebook for disaster recovery and business continuity is also available for purchase. In June 2002, the National Institute of Standards and Technology (NIST) plans to publish a "Contingency Planning Guide for Information Technology Systems." The document will be posted at http://csrc.nist.gov. The State of Texas has published a lengthy guideline for business continuity planning, which is described below. The document is available at: www.dir.state.tx.us/security/policies/index.html.

"The Information Resources Asset Protection Council (IRAPC) was a forum for agencies and universities to seek solutions in areas of resource protection through cooperative efforts and information sharing. In 1997, over ten agency and university representatives formed a special IRAPC team and began writing business continuity planning guidelines. These guidelines were presented to the Department of Information Resources (DIR) for publication. This document is a result of that special team's efforts."

C. Homeland Security Initiatives

Ken Hassler and Dan Davis described the process for developing a "Continuity of Operations Plan" that the federal government uses. The plan assumes a worst-case scenario, but can be used for less severe situations. A worst-case scenario assumes working in an austere environment, where nothing is taken for granted, including basics such as electricity, purchasing procedures, provisions for personnel and even chain-of-command. The key to a business continuity plan is phased implementation, because the plan will identify gaps and weaknesses that exceed available resources. Training is an essential component. States face a dual challenge, because they must provide support for the disaster response as well as setting up new operations. Some federal agencies are implementing the concept of an alternate command post, which they are staffing on a rotating basis.

D. Discussion of Disaster Recovery and Business Continuity

Participants engaged in a wide-ranging discussion of issues pertaining to disaster recovery and business continuity. Comments are summarized below.

A State Emergency Operations Plan (SEOP) exists, which describes how the state will respond to a disaster. The Homeland Security Leadership Group will conduct a training exercise for all participants in the plan. One outcome may to identify the need to address continuity of government operations, which is not covered in the current plan. Presently, only NEMA has an alternate site for operations, although the original layout of State's Emergency Operations Center had office space for several agencies. The SEOP also addresses chain of command and continuity of government authority.

Four agencies are planning a combined Emergency Operations Center at the National Air Guard Base. The combined EOC will serve as a communications center, only, for NEMA, the National Guard, State Patrol and Department of Roads.

Budget issues are a constraint for both planning and implementation. Many agencies do not have the resources to engage in a planning process for disaster recovery and business continuity. A multi-year strategy will be needed for implementation.

Information technology is essential to many aspects of Homeland Security. Federal funding for Homeland Security may be available for IT disaster recovery, and the IT perspective should be part of the exercise design team for testing the SEOP.

Communication and cooperation among agencies may provide low cost solutions to some aspects of disaster recovery. For example, one agency's training rooms could provide temporary office space for another agency in an emergency. Few, if any, agencies can afford hot, warm, or even cold back-up facilities for computer systems. But working together, agencies could serve this function for each other. At a minimum, agencies can create a template and scenarios that all agencies could follow

when developing disaster recovery and business continuity plans. For example DOR is working on a scenario that assumes destruction of their computer room.

Information Management Services has an existing cold site, which was OK for the 1980's but is no longer adequate for current or future trends in computer needs of users. Some private companies have established regional computing facilities, which can all assume the role of headquarters. This is one way to have multiple hot or warm sites available, without major additional costs. The key to alternate sites is that they must also serve a day-to-day operational need.

The magnitude of business continuity and disaster recovery requires a long-term effort that begins with picking a slice and working on it. The entire effort will be a multi-year phased implementation, especially in light of the severe budget and resource constraints that agencies face. Several steps include:

- Develop a template for disaster recovery and business continuity plans;
- Mesh IT disaster recovery with Homeland Security planning;
- Evaluate the potential role of the emergency communications center that DOR, NEMA, NNG, and NSP are planning;
- Brief policy makers on the status of disaster recovery and business continuity plans for information technology.

Several of those present volunteered to work on this topic, including Dwayne Dvorak, Ron Woerner, Scott Evers, Allan Albers (or designee), Scott McFall, and Jerry Hielen. Steve Schafer will facilitate the group to get it started. Participation on the group is open. Their immediate task is to prepare a template for developing disaster recovery and business continuity plans. Their first meeting will be Tuesday June 11, 2002.

E. Update on Other Security Initiatives

1. Security Awareness Day. Ron Woerner described plans for this event, which will be July 15 at the DOR auditorium. Winn Schwartau will be the keynote speaker.
2. Enterprise Security Awareness Training. Jerry Hielen described their efforts to develop security training.
3. IMServices Security and Directory Services Study. Jerry Hielen and Steve Hartman gave an update on directory services study. The consultant is preparing a report and will soon set up a test environment.

F. Update on Security Assessment RFP

Steve Schafer explained that the RFP was close to completion. As soon as it is ready, he will share it with all agencies that are affected.

G. Other Implementation Issues

1. Business Case Outline
2. Other topics

H. Next Meeting Date

The work group will meet again on Tuesday, June 11, 2002, from 1:30 to 3:30 at NSOB LLF. The agenda will focus on developing a template for preparing disaster recovery plans.